Homepage
News
Features & Contents
From the Editor
Events
Links
Bookstore
Magazine Information
Magazine Registration
Advertising Information
Enewsletter
Contact

Privacy Policy
Terms & Conditions

08 October 2004

Top 20 threats unveiled

Sarah Hilley

Government security agencies and the SANS training institute have revealed the top 20 dangerous Internet vulnerabilities of 2004.

The flaws are divided up into UNIX and Windows categories and cover severe and prevalent holes.

Around 60% of last year s vulnerabilities have still retained their place in the list for 2004. However, new types of technologies such as instant messaging have penetrated the top 20.

"As Microsoft bundles its instant messenger program with XP, we ve seen a big prevalence in IM apps, which opens up new risks, said Ross Patel, Editor Top-20 2004.

"These new technologies have been evolving over the past year and are in the mindset of hackers, said Gerhard Eschelbeck, CTO Qualys.

A new category of kernel operating system vulnerabilities has also been selected for the UNIX list. This is a threat which is often overlooked, said Eschelbeck. It involves attacking the core of the OS, which gives easy access to everything.

A more specific threat, the LSAS vulnerability, which was exploited by the Sasser worm in May, has been given prominence. There are still many unpatched systems for this flaw so we had to give it attention, explained Eschelbeck.

Not all of the decisions to include certain vulnerabilities were so clear cut, however.
Patel said that the inclusion of the database category in the UNIX list was a higly contested decision, while the listing of Web servers was an obvious winner.

Strangely the category containing the recent Microsoft JPEG flaw has been omitted.
Eschelbeck warns that this flaw is very likely to be the target of an automatic worm soon.

He said the top 20 list is designed to be the first layer of defence that organizations need to take to patch systems.

The list was compiled by the National Infrastructure Security Co-ordination Centre (NISCC), Department of Homeland Security (DHS), Federal Bureau of Investigation(FBI) and Public Safety and Emergency Preparedness Canada (PSEPC)among others.

Qualys has made a free vulnerability scanner dedicated to the top 20 list available for download at: https://sans20.qualys.com

And the vulnerability categories are &

Windows:

1 Web servers & Services
2 Workstation Service
3 Windows Remote Access Services
4 Microsoft SQL Server (MSSQL)
5 Windows Authentication
6 Web browsers
7 File-sharing applications
8 LSAS Exposures
9 Mail Client
10 Instant Messaging

UNIX:

1 BIND Domain Name System
2 Web Server
3 Authentication
4 Version Control Systems
5 Mail Transport Service
6 Simple Network Management Protocol (SNMP)
7 Open Secure Sockets Layer (SSL)
8 Misconfiguration of Enterprise Services NIS/NFS
9 Databases
10 Kernel

Back to news index